Ministerie van Veiligheid en Justitie

Directie Wetgeving

Contactpersoon
T 070 370 79 11
F 070 370 79 10

Datum
29 april 2011

Ons kenmerk
5688920/11/6

Datum vaststelling
29 april 2011

bijlage

Notitie privacybeleid

Bijlage nummer	1
Horend bij	Brief van de Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties

Notitie privacybeleid

Samenvatting

In deze notitie geeft het kabinet allereerst een overzicht van de maatregelen op het gebied van gegevensverwerking en gegevensbescherming ter uitvoering van het regeerakkoord. Daarnaast geeft het kabinet, op verzoek van de Tweede Kamer, een nadere visie op de Europese en internationale ontwikkelingen op het gebied van de gegevensverwerking. Vervolgens geeft het kabinet een stand van zaken weer van de uitvoering van een kabinetsstandpunt naar aanleiding van de evaluatie van de Wet bescherming persoonsgegevens en het advies van de Adviescommissie veiligheid en de persoonlijke levenssfeer. Verder wordt in deze notitie, naar aanleiding van verzoeken van de Tweede Kamer, ingegaan op enkele brieven die de Kamer mocht ontvangen, van onder meer het College bescherming persoonsgegevens.

Inleiding

Privacybeleid, regeerakkoord en andere beleidsinitiatieven

In het regeerakkoord "Vrijheid en verantwoordelijkheid" van 30 september 2010 wordt op verschillende plaatsen krachtig ingezet op meer aandacht voor de informatiebeveiliging en de bescherming van persoonsgegevens. De voornemens in het regeerakkoord hebben zowel betrekking op de verwerking als op de bescherming van persoonsgegevens.

De *verwerking* van persoonsgegevens kan in de visie van het kabinet een belangrijke ondersteuning betekenen van een beleid dat is gericht op bevordering van de veiligheid in de openbare ruimte. Zo heeft het kabinet meer cameratoezicht in het vooruitzicht gesteld. Ook wordt de toepassing van ANPR (automatische nummerplaatherkenning) ten behoeve van de opsporing nader genormeerd. Nadere voorstellen volgen voor een bredere toepassing van ANPR.

De *bescherming* van persoonsgegevens kan in de visie van het kabinet worden verbeterd.

Het kabinet heeft verschillende maatregelen in het vooruitzicht gesteld. Allereerst zullen alle voorgenomen maatregelen die de opslag, de koppeling en de verdere verwerking van persoonsgegevens behelzen bij de voorbereiding nadrukkelijk meer worden getoetst aan de effectiviteit. Voorgenomen maatregelen zullen bovendien zoveel mogelijk worden voorzien van een horizonbepaling. Daarnaast komt er een verplichting om in gevallen van verlies, diefstal of misbruik van persoonsgegevens melding te maken van dat voorval aan de toezichthouder. De toezichthouder kan boetes opleggen indien de meldplicht niet wordt nageleefd. Verder zal het toezicht op grootschalige informatiseringsprojecten en het oplossen van automatiseringsproblemen structureel worden aangescherpt. Tenslotte komt het kabinet met een integrale aanpak van cybercrime. De invulling van elk van deze gegevens wordt hierna toegelicht.

Ook op Europees niveau zal het kabinet zich inzetten voor het bereiken van de in het regeerakkoord geformuleerde doelen. Op 4 november 2010 heeft de Europese Commissie een *Mededeling over "Een integrale bescherming van persoonsgegevens in de Europese Unie"* vastgesteld. Een eerste inhoudelijke beoordeling van die mededeling in de vorm van een BNC-fiche is de Tweede Kamer aangeboden bij brief van 21 december 2010 van de Staatssecretaris van Buitenlandse Zaken (Kamerstukken II 2010/11, 22 112, nr. 1116). De mededeling wijst de weg naar een modernisering van het gegevensbeschermingsrecht van de Europese Unie dat samen met artikel 10 van de Grondwet de basis vormt voor onze nationale wetgeving op het gebied van de bescherming van persoonsgegevens.

Het vorige kabinet heeft bij brief van 9 november 2009 van de toenmalige Ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties aan de Voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II 2009/10, 31 051, nr. 5) een *kabinetsstandpunt* toegezonden naar aanleiding van de rapporten over de *evaluatie van de Wet bescherming persoonsgegevens (Wbp)* en het *rapport van de Adviescommissie veiligheid en de persoonlijke levenssfeer*. In dat kabinetsstandpunt is een aantal voornemens tot wetgeving aangekondigd die nog niet zijn uitgevoerd.

Bij de behandeling van de begroting van het Ministerie van Veiligheid en Justitie in de Tweede Kamer op 24 november 2010 is door de eerste ondergetekende de toezegging gedaan een nadere visie te geven op het integraal privacybeleid, waarbij is aangegeven dat zoveel mogelijk rekening wordt gehouden met de Europese ontwikkelingen ter zake. Met deze brief geven wij uitvoering gegeven aan die toezegging.

Bij brief van 13 januari 2011 heeft de eerste ondergetekende u toegezegd in deze notitie nog een reactie te geven op het schrijven van het College bescherming persoonsgegevens (Cbp) van 6 december 2010 aan de leden van de Vaste Commissie voor Veiligheid en Justitie.

Bij brief van 15 februari 2011 heeft de Vaste Commissie voor Binnenlandse Zaken de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Veiligheid en Justitie verzocht te reageren op een onderzoek van Privacy International over de stand van zaken over de privacy in Nederland. Wij geven in deze notitie een korte reactie op dat onderzoek.

Tenslotte heeft de eerste ondergetekende tijdens het algemeen overleg dat op 17 februari 2011 plaatsvond over de JBZ Raad van 24 en 25 februari 2011 aangekondigd dat in deze notitie nog op een aantal specifieke onderwerpen die door de leden van de fractie van D66 zijn genoemd zal worden ingaan.

Doel van deze notitie

Met deze notitie beoogt het kabinet vooral zo concreet mogelijk aan te geven hoe het regeerakkoord, de Europese ontwikkelingen en de voornemens in het kabinetsstandpunt zich tot elkaar verhouden. Daarbij wordt aangegeven wat op korte termijn wordt aangevat in de vorm van wetgeving, welke onderdelen van het regeerakkoord dit betreft, wat bij de voorbereiding van wetgeving ook wordt meegenomen van hetgeen nog moet worden uitgevoerd, en wat daarvan bij nadere afweging - gelet op de verwachte ontwikkelingen in Europa - niet zal worden meegenomen.

De nadere visie van het kabinet is dus vooral gericht op *uitvoering* in de vorm van wetgeving op zo kort mogelijke termijn van hetgeen in het regeerakkoord is opgenomen en van een aantal eerder voorgenomen maatregelen. Wat visievorming voor het overige betreft, geeft het kabinet in deze notitie aan hoe het aankijkt tegen de door het vorige kabinet vastgestelde standpunt over de toekomst van de Wbp op de kortere termijn en de verhouding van de Wbp tot het veiligheidsdomein. Het huidige kabinet ziet het als prioriteit om een aantal maatregelen uit dat standpunt daadwerkelijk uit te voeren. Dit kabinet heeft niet de behoefte op deze punten weer met een nieuwe beleidsvisie te komen. Dat doet het kabinet niet alleen omdat het de bestaande problemen met de Wbp onderkent en de oplossingsrichting daarvoor in grote lijnen onderschrijft, maar ook omdat in Europa inmiddels stappen worden gezet die van grote invloed zijn op de mogelijkheden om in Nederland eigen wetgeving tot stand te brengen op het gebied van de bescherming van persoonsgegevens. Op die Europese initiatieven heeft het kabinet een visie die de Kamer inmiddels in de vorm van het BNC-fiche heeft ontvangen. Op een enkel onderdeel van die Europese initiatieven geeft het kabinet een aanvullende visie, omdat dit buiten het kader valt van hetgeen normaliter in een BNC-fiche wordt verantwoord.

Deze notitie richt zich vooral op het recht inzake de bescherming van persoonsgegevens en enkele direct daarmee samenhangende aspecten van informatiebeveiliging. De aanpak van grootschalige automatiseringsprojecten, het oplossen van automatiseringsproblemen en de aanpak van cybercrime valt buiten het kader van deze notitie. Wat de bestrijding van cybercrime betreft, heeft de Minister van Veiligheid en Justitie inmiddels bij brief van 22 februari 2011 aan de voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II 2010/11, 26 643, nr. 174) de Nationale Cyber Security Strategie gepresenteerd.

Uitvoering regeerakkoord

Cameratoezicht en automatische nummerplaatherkenning

Het bevorderen van het feitelijk gebruik van het algemene cameratoezicht is vooral een kwestie van aanpak door decentrale overheden en particuliere belanghebbenden zelf. In de sfeer van de regelgeving zal het kabinet echter nog een voornemen uitvoeren. In de Gemeentewet staat dat camerabeelden gedurende vier weken mogen worden bewaard. Voor de private toepassing van

cameratoezicht ontbreekt een specifieke regeling en moet worden teruggevallen op de algemene regeling van de Wet bescherming persoonsgegevens. In het Vrijstellingsbesluit Wbp is een regeling opgenomen die verantwoordelijken vrijstelt van de verplichting hun gegevensverwerking voor bewakings- en beveiligingsdoeleinden te melden bij het Cbp, onder de voorwaarde dat camerabeelden aan een beperkte bewaartermijn van slechts 24 uur zijn onderworpen. Het ligt in de bedoeling om op korte termijn een reeds in consultatie gegeven wijziging van het Vrijstellingsbesluit Wbp aan de ministerraad voor te leggen met het doel om de bewaartermijn voor deze camerabeelden gelijk te trekken met de bewaartermijn voor camerabeelden uit het publieke domein. Op die manier kunnen burgers en bedrijven zonder onderworpen te zijn aan de administratieve last van de melding beter en meer afgewogen zelf beoordelen of zij deze beelden gebruiken voor het verbeteren van hun eigen veiligheid of voor het doen van aangifte van op de beelden geconstateerde strafbare feiten.
Met betrekking tot automatische nummerplaatherkenning (ANPR) door de politie heeft de Minister van Veiligheid en Justitie een wetsvoorstel in consultatie gegeven tot wijziging van het Wetboek van Strafvordering waarin een solide regeling wordt voorgesteld voor het bewaren van kentekengegevens voor de opsporing van strafbare feiten en de aanhouding van voortvluchtige personen. Hierin is voor de duur van de bewaartermijn aangesloten bij de hiervoor genoemde termijn van vier weken.

Toetsing voorgenomen maatregelen gegevensverwerking

Nieuwe voorgenomen wettelijke maatregelen die gericht zijn op de invoering en rechtvaardiging van nieuwe grootschalige verwerkingen van persoonsgegevens door de overheid zullen nadrukkelijker dan voorheen het geval is moeten worden getoetst op effectiviteit. Over de technische en informationele effectiviteit moet op transparante wijze verantwoording worden afgelegd. Ook de vraag of een nieuw systeem in alle opzichten voldoet aan de eisen die voortvloeien uit Europees en internationaal recht en uit de Wbp behoort daarbij telkens onder ogen te worden gezien. Uit oogpunt van goede wetgeving zullen de ministeries van Veiligheid en Justitie en Binnenlandse Zaken en Koninkrijksrelaties daarop toezien. Bij die toetsing komt ook aan de orde of het wetsvoorstel ten minste voorzien is van een evaluatiebepaling, en of het opnemen van een horizonbepaling aan de orde is. Of een horizonbepaling moet worden vastgesteld is mede afhankelijk van mate en de aard van de inmenging in de rechten op bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens, en daarnaast van de investeringen die met de voorgenomen maatregelen zijn gemoeid. Dit zal van geval tot geval moeten worden vastgesteld. In het hierboven genoemde wetsvoorstel tot regeling van de ANPR is zowel een horizonbepaling als een evaluatiebepaling opgenomen.

Meldplicht datalekken

De laatste jaren hebben zich in het ons omringende buitenland met een zekere regelmaat ernstige incidenten voorgedaan waarbij grote hoeveelheden persoonsgegevens in het openbare domein zijn gebracht als gevolg van ontoereikend gebleken beveiligingsmaatregelen. Zulke incidenten kunnen zich ook in Nederland voordoen. Op grond van artikel 13 van de Wbp is de verantwoordelijke voor een verwerking van persoonsgegevens verplicht om passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige

verwerking. De Wbp regelt thans niet welke feitelijke gevolgen moeten worden verbonden aan gevallen waarin sprake is van verlies of onrechtmatig gebruik van persoonsgegevens als gevolg van ontoereikend gebleken beveiligingsmaatregelen.
In het wetsvoorstel tot wijziging van de Telecommunicatiewet in verband met de implementatie van het gewijzigd Europees regelgevend kader voor elektronische communicatie (NRF) (Kamerstukken II 2010/11, 32 549, nr. 1-3) is een verplichting opgenomen voor de aanbieders van elektronische communicatienetwerken en -diensten om de persoonsgegevens en de persoonlijke levenssfeer van de abonnee of gebruiker beter te beschermen tegen inbreuken op de veiligheid van persoonsgegevens en de ongunstige gevolgen die dit kan hebben voor de persoonlijke levenssfeer van degene wiens persoonsgegevens het betreft. Indien zich een dergelijke inbreuk voordoet heeft de aanbieder van een openbare telecommunicatiedienst de verplichting die inbreuk, onverwijld nadat hij die inbreuk heeft geconstateerd, te melden bij de toezichthouder. Ingeval de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens en de persoonlijke levenssfeer van degene wiens persoonsgegevens het betreft, dient de aanbieder van de telecommunicatiedienst of het -netwerk degene wiens persoonsgegevens het betreft onmiddellijk in kennis te stellen van de inbreuk en hem te informeren over de eventuele middelen die de eindgebruiker zelf kan treffen om de risico's die hieruit voortvloeien tegen te gaan.
In het regeerakkoord is aangegeven dat een dergelijke meldplicht zich ook moet uitstrekken over alle diensten van informatiemaatschappij, de overheid daaronder begrepen. Bij de behandeling van het kabinetsstandpunt in de Tweede Kamer is door het vorige kabinet reeds toegezegd dat deze meldplicht ook in de Wbp zou worden opgenomen. Het regeerakkoord sluit bij dit voornemen aan.
In een wetsvoorstel dat medio 2011 in consultatie zal gaan zal een dergelijke verplichting worden opgenomen. De meldplicht zal tweeledig zijn. Enerzijds zal de meldplicht moeten worden nagekomen met het oog op de belangen van betrokkenen. Anderzijds zal de meldplicht moeten worden nagekomen met het oog op de handhaving. Dat betekent dat zowel de betrokkenen als de toezichthouder zullen moeten worden ingelicht. Een nadere begrenzing van de meldplicht zal noodzakelijk zijn om meldingen van bagatelzaken tegen te gaan. Dit is van belang, aangezien de administratieve lasten en de nalevingskosten gemoeid met deze maatregel, zo beperkt mogelijk moeten blijven. Dat betekent dat de precieze inhoud van de melding en wijze van melden aandacht verdient. Daarnaast moet worden bezien of er redenen zijn de meldplicht ten opzichte van de toezichthouder te differentiëren van de meldplicht ten aanzien van betrokkenen. Ook zal nog moeten worden nagegaan hoe de meldplicht zich verhoudt tot de aansprakelijkheid van de verantwoordelijke.
De reikwijdte van deze meldplicht verdient afzonderlijke aandacht. Voorop staat dat de regeling in de Telecommunicatiewet, zoals aangevuld met het vorenbedoelde wetsvoorstel, onverkort gehandhaafd blijft. Dat is noodzakelijk om de desbetreffende EU-besluiten herkenbaar te implementeren en het daarmee verband houdende begrippenapparaat van de Telecommunicatiewet niet te compliceren. De meldplicht voor datalekken zal voor alle andere gevallen worden opgenomen in hoofdstuk 5 van de Wbp. Aangezien de verplichtingen uit deze laatste wet zich richten tot de "verantwoordelijke" (dat is de partij die het doel en de middelen voor een gegevensverwerking vaststelt), ligt het voor de hand dat de meldplicht wordt gelegd op de verantwoordelijke. Dit heeft wel tot consequentie dat de kring van partijen tot wie de verplichting zich richt niet per definitie gelijk is aan de aanbieders van diensten "van de informatiemaatschappij", zoals bedoeld in het regeerakkoord. Het is echter buiten twijfel dat die dienstaanbieders zodra

zij persoonsgegevens verwerken als verantwoordelijke in zin van de Wbp moeten worden aangemerkt.
Verder is het zo dat gegeven de wettelijk geregelde verhouding tussen de verantwoordelijke en de bewerker (dat is een partij aan wie een gegevensverwerking wordt uitbesteed) de verantwoordelijkheid voor het naleven van de meldplicht ook bij de verantwoordelijke blijft berusten in de gevallen waarin sprake is van uitbesteding.
De meldplicht zal worden gesanctioneerd met een punitieve sanctie. Daarbij ligt de bestuurlijke boetebevoegdheid het meest in de rede. Die sanctionering staat niet op zichzelf. Ook dit kabinet onderschrijft het voornemen de sanctionering van de gegevensbeschermingswetgeving kwalitatief te versterken.

Aanpak sanctionering overtredingen Wet bescherming persoonsgegevens

Tot dusverre is het opleggen van een bestuurlijke boete door het Cbp alleen mogelijk wanneer administratieve verplichtingen van de Wbp niet worden nagekomen. De keuze om handhaving van de meldplicht voor datalekken te sanctioneren met een bestuurlijke boete roept de vraag op of dit handhavingsinstrument een bredere toepassing verdient. In het meergenoemde kabinetsstandpunt is al aangegeven dat het voornemens was om de handhaving van de Wbp te versterken door ook de materiële bepalingen van die wet te sanctioneren met behulp van een bestuurlijke boete. Ook zal de strafrechtelijke sanctionering opnieuw worden bezien. Dit voornemen wordt thans ten uitvoer gelegd in het hierboven bedoelde wetsvoorstel.
Bij de uitwerking van dit voornemen dienen een aantal nadere keuzes te worden gemaakt. Zo moet allereerst worden vastgesteld welke onderdelen van de Wbp voor een sanctionering met een bestuurlijke boete in aanmerking komen. Dat zijn in ieder geval de normen van de Wbp die rechtstreeks verplichtingen leggen op de verantwoordelijke en de normen die een verbod inhouden. Daarbij moet ook rekening worden gehouden met de belangen van de bestrijding van fraude en andere criminaliteit. Nadere besluitvorming terzake moet uit oogpunt van uitvoerbaarheid en handhaafbaarheid in samenspraak met het Cbp plaatsvinden.
De normen van de Wbp zijn, zoals bekend, abstract geformuleerd. Dat roept voor de wetgever en handhaver wel de verplichting op om zoveel mogelijk duidelijkheid te verschaffen over de vraag of een bepaald handelen of nalaten in strijd is met de Wbp. Aan de normen van de Wbp zal inhoudelijk weinig kunnen worden veranderd. Zij zijn gebaseerd op richtlijn nr. 95/46/EG, de EU-privacyrichtlijn.
In de afgelopen jaren zijn deze normen nader ingevuld door de jurisprudentie van het Hof van Justitie van de Europese Unie. De opinies van de samenwerkende privacytoezichthouders van de EU, de artikel 29 Werkgroep, kunnen behulpzaam zijn bij een verdere duiding van de relevante normen. Ook op nationaal niveau is er inmiddels jurisprudentie tot stand gekomen. Daarnaast zijn de normen van de Wbp aangevuld met specifieke wettelijke regels voor specifieke toepassingen. Er is ook een vaste toepassingspraktijk van het Cbp.
Niettemin zal zich van tijd tot tijd de noodzaak voordoen dat het Cbp met behulp van boeterichtsnoeren zo nauwkeurig mogelijk nader aangeeft in welke categorieën van gevallen er handhavend moet worden opgetreden. Het Cbp wordt dan ook uitgenodigd daarvoor in aanmerking komende onderwerpen mee te delen en daarbij aan te geven wanneer de daarvoor benodigde richtsnoeren zullen worden vastgesteld, zodat in de memorie van toelichting bij het wetsvoorstel waarin de sanctionering wordt geregeld zoveel mogelijk duidelijkheid kan worden

gegeven. Verwacht mag worden dat die nader invulling door het Cbp ook een zekere prioritering van zaken, zoals het Cbp die ziet, weerspiegelt.
Verder zal nog moeten worden vastgesteld welk boetemaximum wordt voorgesteld. Een boetemaximum moet maatschappelijk gezien aanvaardbaar zijn en in verhouding tot de aard van de normen proportioneel zijn. In samenhang met de vaststelling van het boetemaximum zal worden bezien of het maximum van de strafrechtelijke boetes moet worden verhoogd. Hoewel in het reeds geruime tijd bij de Tweede Kamer aanhangige wetsvoorstel tot wijziging van de Wbp in verband met de vermindering van administratieve lasten (Kamerstukken II 2008/09, 31 841, nr. 2) een verhoging van de geldboetecategorieën is opgenomen, is het verstandig het maximum van strafrechtelijke en de bestuursrechtelijke boete zoveel mogelijk te harmoniseren.

Tenslotte zal in een wetsvoorstel worden geregeld dat bezwaar en beroep wordt opengesteld tegen een definitief rapport van bevindingen, in de zin van artikel 60 van de Wbp. Dat biedt verantwoordelijken de gelegenheid om desgewenst het oordeel van de rechter in te winnen over feiten die door het Cbp zijn verzameld en de kwalificatie die het Cbp daaraan geeft. Op deze wijze worden de "checks and balances" in de Wbp uitgebreid. Dit is niet alleen voor verantwoordelijken van belang, het is ook voor het Cbp van belang. Immers, het kan in een bezwaarschriftprocedure zonodig tot heroverweging overgaan.
Uiteraard is bezwaar en beroep tegen een besluit tot oplegging van een bestuurlijke boete mogelijk.

Gegevens delen ten behoeve van het voorkomen van overlast, huiselijk geweld en criminaliteit

Het regeerakkoord vermeldt dat daders in hun eigen omgeving moeten worden aangepakt. Veiligheidshuizen spelen hierbij een belangrijke rol. De veiligheidshuizen, samenwerkingsverbanden van verschillende organisaties, gaan dadergericht te werk bij het terugdringen van overlast, huiselijk geweld en criminaliteit. De voordelen van deze wijze van preventief werken hebben tot goede resultaten geleid. De veiligheidshuizen zullen worden voortgezet en verder ontwikkeld.
Het kabinet staat een dadergerichte aanpak voor om ernstige overlast, huiselijk geweld en criminaliteit terug te dringen. Deze aanpak is gericht op een combinatie van preventie, repressie en zorg en krijgt concreet vorm in samenwerkingsverbanden, zoals het Veiligheidshuis en de Netwerk- en trajectberaden nazorg jeugd. Hier komen partners vanuit verschillende disciplines (zorg, hulpverlening, gemeente, justitie) bij elkaar en wordt op basis van de ernst van het gedrag en de onderliggende problematiek bepaald welk traject wordt ingezet om overlastgevend of crimineel gedrag te voorkomen of aan te pakken. Deze werkwijze kan alleen plaatsvinden als relevante informatie wordt gedeeld tussen de deelnemende partners. Deze informatie moet niet alleen lokaal maar ook landelijk kunnen worden gedeeld, aangezien hardnekkige overlastgevers en criminelen zich vaak bewegen over meerdere regio's. Ook hier geldt dat deze informatie-uitwisseling zorgvuldig moet plaatsvinden, overeenkomstig het in de paragraaf *Helpdesk voor professionals in veiligheid en justitiële jeugdzorg* van deze brief geschetste 6-stappenplan. Deze informatie-uitwisseling vindt zoveel mogelijk plaats met toepassing van de bestaande regels voor samenwerkingsverbanden op grond van de Wbp, de Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens en de Wet op de jeugdzorg. Echter, wanneer blijkt dat deze regelgeving onvoldoende ruimte zou bieden voor

structurele en niet-vrijblijvende informatie-uitwisseling binnen netwerkverbanden zoals het Veiligheidshuis, zal het kabinet zonodig initiatieven nemen om de daarvoor in aanmerking komende regelgeving aan te passen. Ook op andere terreinen van de rechtshandhaving is het delen van juiste informatie tussen de juiste betrokkenen essentieel voor de effectiviteit van de handhaving. Fraude- en criminaliteitsbestrijding is daarvan een prominent voorbeeld. Ook hier zal het kabinet zonder aarzelen initiatieven nemen tot aanpassing van de daarvoor in aanmerking komende regelgeving, wanneer zou blijken dat die regelgeving tekortschiet om de effectiviteit van de handhaving te bewerkstelligen.

Europese en internationale ontwikkelingen

Bij meergenoemde brief van 21 december 2010 heeft de Staatssecretaris van Buitenlandse Zaken aan de Voorzitter van de Tweede Kamer een BNC-fiche aangeboden waarin een eerste beoordeling door het kabinet is neergelegd van de Mededeling van de Europese Commissie van 4 november 2010, COM (2010) 609 def., "Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie". In het BNC-fiche is puntsgewijs aangegeven wat de reactie van het kabinet is op de diverse onderdelen van de visie en de voornemens van de Commissie.
In grote lijnen kan het kabinet zich vinden in de uitgangspunten van de mededeling. Ook het kabinet is van oordeel dat de beide uitgangspunten van de EU-privacyrichtlijn, het garanderen van een hoog niveau van de bescherming van het recht op gegevensbescherming en het garanderen van een vrij verkeer van persoonsgegevens binnen de EU, nog onverkort geldend zijn. Het is, ook in de visie van het kabinet, een juiste analyse dat de ontwikkeling van de technische mogelijkheden, en de mede daaruit voortvloeiende globalisering, hebben geleid tot veranderingen. Die veranderingen bestaan hierin dat gegevens wereldwijd worden verwerkt voor de meest uiteenlopende doeleinden en dat dit op een steeds geavanceerdere wijze en tegen steeds lagere kosten mogelijk is. De wereldwijde dimensie van die ontwikkeling maakt dat het steeds moeilijker wordt om vast te stellen welk recht van toepassing is op de gegevensverwerking, omdat verschillende aspecten van die verwerking aanknopingspunten hebben met verschillende rechtsstelsels binnen en buiten de EU. Cloudcomputing is daarvan het beste voorbeeld. Hoewel cloudcomputing en "software as a service" voor het bedrijfsleven grote voordelen biedt in de vorm van gebruiksgemak en lagere kosten, is ook aannemelijk is dat de risico's voor de bescherming van de persoonsgegevens door cloudcomputing toenemen. Wanneer Europese burgers voor de handhaving van de hun toekomende rechten afhankelijk zijn van verantwoordelijken die zich buiten de EU bevinden roept dit de vraag op aan welk rechtsstelsel voor de bescherming van persoonsgegevens die verantwoordelijken zijn onderworpen. Niet vanzelfsprekend is dat die verantwoordelijken de op hen rustende verplichtingen nakomen op een niveau vergelijkbaar met het niveau dat in de EU geldt. Ook kan niet worden gegarandeerd dat de rechten op inzage, correctie, afscherming en verzet in dergelijke situaties volledig tot gelding kunnen worden gebracht.
De omvang en aard van deze problemen zijn zodanig dat een oplossing daarvan op nationaal niveau niet goed mogelijk is. Uiteindelijk zullen daarvoor alleen op mondiaal niveau oplossingen kunnen worden gevonden. De EU heeft de ambitie om daarin een belangrijke rol te spelen. Het kabinet onderschrijft dit. Het kabinet streeft er daarom naar op het niveau van de EU, overeenkomstig artikel 16 van het Verdrag betreffende de werking van de Europese Unie, oplossingen voor deze problemen voor te stellen en uit te werken.

Daarbij moet wel worden vastgesteld dat een oplossing van al die problemen op korte termijn niet kan worden verwacht, noch op EU-niveau, noch op mondiaal niveau. De oorzaken daarvoor zijn tweeërlei. Allereerst is voldoende duidelijk dat de technische ontwikkelingen op ICT-gebied onverminderd doorgaan en dat steeds moet worden bezien of op nieuwe ontwikkelingen een reactie in de vorm van wetgeving nodig is. Daarnaast is de benadering van het gegevensbeschermingsrecht in de EU nogal verschillend van de benadering van dat recht in andere delen van de wereld. De EU formuleert een grondrecht op de bescherming van persoonsgegevens. In de Verenigde Staten en in Azië is het recht op bescherming van persoonsgegevens veel meer ingebed in de diverse rechtsgebieden die onderdeel zijn van het privaatrecht. Dit leidt tot belangrijke verschillen op het gebied van toezicht op de naleving, handhaving en sanctionering tussen de werelddelen.
Om die redenen is het niet verwonderlijk dat ook de Commissie in de mededeling niet in staat is om kant en klare oplossingen te formuleren, maar dat een aantal onderwerpen nog nadere studie verdienen. Het kabinet is wel van mening dat op sommige onderdelen wel beslissingen genomen hadden kunnen worden. Zo is het kabinet teleurgesteld dat in de mededeling geen uitsluitsel wordt gegeven over de keuze van het instrument waarin de wetgevingsvoornemens worden neergelegd, namelijk een richtlijn, een verordening of een combinatie van beide. Ook op het gebied van de terugdringing van de administratieve lasten had de Commissie naar het oordeel van het kabinet de keuze kunnen maken om de bestaande instrumenten als de verplichting tot het melden van elke gegevensverwerking en het voorafgaand onderzoek af te schaffen of te behouden.
Het kabinet herkent overigens de vijf voornaamste knelpunten die de Commissie in de mededeling heeft geïdentificeerd. Het betreft de omgang met de gevolgen van nieuwe technologieën, de noodzaak tot uitwerking van de internemarktdimensie, verbetering van de mogelijkheden voor internationale gegevensdoorgifte, effectievere handhaving van het gegevensbeschermingsrecht en meer samenhang in het wettelijk kader. Zoals verantwoord in het BNC-fiche betekent dit niet dat het kabinet ook zonder meer met alle onderdelen van de mededeling instemt. Voor de details verwijst het kabinet naar het fiche.
Naar aanleiding van een vraag van de leden van de fractie van D66 tijdens het algemeen overleg van 17 februari 2011 over de JBZ Raad van 24 en 25 februari 2011 over de positie van collectiefbelangacties in het privacyrecht, verwijst het kabinet naar het meergenoemde BNC-fiche. Kort weergegeven staat daarin dat het kabinet niet afwijzend staat tegenover de introductie van deze acties, maar dat dit alleen onder voorwaarden acceptabel is. Het kabinet is geen voorstander van de mogelijkheid om met een dergelijke actie schadevergoeding in geld te vorderen. Verder moet de in rechte optredende organisatie een zekere legitimiteit bezitten en is een behoorlijke regeling van het procesrecht nodig.

Tenslotte is het waard te vermelden dat ook de Raad van Europa nog een initiatief heeft genomen. Aangekondigd is dat het op 28 januari 1981 te Straatsburg tot stand gekomen Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Trb. 1988, 7) - ook wel bekend als Verdrag nr. 108, of het Dataprotectieverdrag - zal worden herzien. In de loop van 2011 kunnen de nodige voorstellen daarvoor worden verwacht. Het kabinet zal vanzelfsprekend ook deze ontwikkeling nauwgezet volgen. Daarbij zet het kabinet in op het garanderen van synergie tussen het Dataprotectieverdrag en het komende nieuwe EU-instrumentarium. Het kabinet acht dit ook van belang met het oog op de implementatie van beide nieuwe instrumenten in de Wbp.

Reactie op de brief van het College bescherming persoonsgegevens van 6 december 2010

Het kabinet beschouwt de brief van het Cbp als een belangrijke ondersteuning van het beleid dat is uiteengezet in het meergenoemde BNC-fiche. Het kabinet wil zich dan ook tot een korte reactie op de vijf hoofdlijnen van de brief beperken.
Wat het versterken van de rechten van burgers door middel van een collectiefbelangactie betreft, is het kabinet het met het Cbp eens dat een dergelijk rechtsmiddel de positie van de betrokkene beslist positief kan beïnvloeden. Zakelijk weergegeven is het Cbp van oordeel dat de Commissie zich actiever zou moeten opstellen om dat recht daadwerkelijk in een nieuwe richtlijn neer te leggen, in plaats van dit slechts te overwegen. Het kabinet heeft in het BNC-fiche echter aangegeven dat er nog wel het nodige zal moeten worden verduidelijkt over de vormgeving van dat recht.
Het kabinet voelt zich gesteund door het Cbp waar het de uitwerking van het beginsel van accountability betreft. Het kabinet is met het Cbp van mening dat wanneer het bedrijfsleven in staat en bereid is volgens de weg van een zo groot mogelijke mate van zelfregulering privacybescherming tot normaal onderdeel van het ondernemingsbeleid te maken, er veel gewonnen wordt voor de gegevensbescherming. Het kabinet zet in de EU gericht in op het bevorderen van dit belang. Op het advies van de Staatscommissie Grondwet om het doelbindingsbeginsel grondwettelijk vast te leggen, hetgeen het Cbp onderschrijft, zal het kabinet afzonderlijk reageren.
Het kabinet is met het Cbp van oordeel dat de gedachte dat "Privacy by design" uitermate geschikt is om bij een technisch ontwerp van meet af aan rekening te houden met de bescherming van de gegevens die op een bepaalde wijze worden verwerkt. Het kabinet zal de toepassing van privacy by design zoveel mogelijk stimuleren.
Mede naar aanleiding van een vraag van de leden van de fractie van D66 op het algemeen overleg van 17 februari 2011 over de JBZ Raad van 24 en 25 februari 2011 onderschrijft het kabinet de gedachte van overkoepelende privacyregulering voor alle sectoren, met inbegrip van politie en justitie, op zichzelf genomen wel, mits op de genoemde terreinen de ruimte bestaat om gelding van dezelfde *beginselen* van gegevensbeschermingsrecht te aanvaarden, maar dat de noodzaak tot afzonderlijke *regels* buiten kijf staat. Het is ondenkbaar dat de transparantieverplichtingen en het inzagerecht op het terrein van politie en justitie op dezelfde wijze worden vormgegeven als voor het overige gegevensbeschermingsrecht.
Tenslotte heeft het kabinet al meermalen aangegeven dat het belang hecht aan de versterking van de toezichthoudende rol van het Cbp. Wat een versterking van de rol van de "Artikel 29 Werkgroep" - het Europees samenwerkingsverband van toezichthouders - betreft, zal het kabinet eerst de concrete voorstellen van de Commissie daarover afwachten, zonder daarop vooruit te lopen.

Kabinetsstandpunt rapporten Adviescommissie veiligheid en de persoonlijke levenssfeer en evaluatie Wet bescherming persoonsgegevens

In dit kabinetsstandpunt zijn door het vorige kabinet verschillende maatregelen in het vooruitzicht gesteld. Een aantal van die maatregelen heeft specifiek betrekking op het gebruik van persoonsgegevens ten behoeve van de veiligheidszorgen en een aantal direct daarmee samenhangende gebieden. Deze maatregelen zijn vooral feitelijk van aard, en niet primair gericht op het

totstandbrengen van regelgeving. Een aantal andere maatregelen hebben betrekking op de bescherming van de persoonlijke levenssfeer in algemene zin. Daar ligt het accent vooral op het actualiseren van de Wbp.

Privacy en veiligheid

Wat de maatregelen op het gebied van de privacy in relatie tot de veiligheidszorg betreft, hecht ook dit kabinet eraan te benadrukken dat bescherming van de persoonlijke levenssfeer en de zorg voor veiligheid van samenleving en individu niet noodzakelijkerwijs tegengestelde belangen zijn die zorgvuldig tegen elkaar moeten worden afgewogen. Het kabinet rekent het tot zijn taak om beide belangen te beschermen. Onder omstandigheden kan de afweging neerkomen op het aanvaarden van een beperking van de persoonlijke levenssfeer ten behoeve van de zorg voor veiligheid van de samenleving. Wettelijke maatregelen op nationaal niveau behoren te zijn voorzien van een transparante toets aan de grondrechten, en adviezen van de daarvoor in het bijzonder in aanmerking komende organisaties. Zoals hierboven reeds aangegeven, zal er bij volgende initiatieven steeds minimaal moeten worden voorzien in een evaluatiebepaling. Een horizonbepaling is een optie voor die gevallen waarin dat gelet op de mate en de aard van de inmenging in de grondrechten en de te plegen investeringen in ICT gerechtvaardigd is. Maar ook hier is enige terughoudendheid geboden.

Gegevens delen ten behoeve van de veiligheid in incidentele gevallen

In het kabinetsstandpunt is het door de Adviescommissie veiligheid en de persoonlijke levenssfeer uitgesproken standpunt onderschreven dat wanneer het noodzakelijk is voor de veiligheid van personen gegevens tussen verantwoordelijken in het overheidsdomein moeten kunnen worden gedeeld, ook in situaties waarin een wettelijke regeling om op structurele basis gegevens te delen nog ontbreekt, en, in uitzonderingsgevallen zonodig zelfs met doorbreking van een wettelijke geheimhoudingsplicht. Ook dit kabinet onderschrijft dat uitgangspunt zeer zeker. Hierboven is al aangegeven dat het kabinet niet zal aarzelen om ten behoeve van de fraude- en criminaliteitsbestrijding wettelijke voorzieningen te treffen om het delen van gegevens tussen toezichthouders en handhavers mogelijk te maken.
In een wetsvoorstel tot aanpassing van de Wbp zal daarnaast een aanvulling op art. 9 Wbp worden voorgesteld om binnen de ruimte die EU-privacyrichtlijn biedt het delen van gegevens mogelijk te maken wanneer het vitaal belang (daaronder wordt verstaan: een onmiddellijke of dreigende aantasting van leven of gezondheid) van de betrokkene of een derde dat vergt. De regeling blijft overigens beperkt tot het regelen van een *bevoegdheid* die alleen bedoeld is voor afzonderlijke en incidentele gevallen van dringende aard. Er heeft zich in het recente verleden een aantal gevallen voorgedaan waarin aan deze bevoegdheid grote behoefte bestond. Te denken valt aan enkele zeer schrijnende gevallen van kindermishandeling en aan de mogelijkheden tot gegevensverwerking ten behoeve van de nabestaanden van de slachtoffers van de vliegramp in Libië.
Op de terreinen waarvoor een aanleiding bestaat om een *verplichting* tot het verstrekken van gegevens vast te stellen, zal in de desbetreffende wetgeving een voorziening moeten worden getroffen. Verplichtingen tot gegevensverstrekking passen niet in het systeem van de Wbp. Dit voorstel sluit overigens inhoudelijk aan bij een reeds in het eerder vermelde wetsvoorstel tot wijziging van de Wbp in verband met de vermindering van administratieve lasten (Kamerstukken II 31841) opgenomen voorziening voor de verwerking van bijzondere

persoonsgegevens ten behoeve van het vitaal belang van een betrokkene of derde.

Gegevens delen ten behoeve van nalevingstoezicht en handhaving op structurele basis

In het kabinetsstandpunt is aangekondigd dat nader wetenschappelijk onderzoek zou worden gedaan naar de mogelijkheden om in de Algemene wet bestuursrecht een voorziening op te nemen om toezichtsgegevens - waaronder mede begrepen persoonsgegevens - op structurele basis te kunnen uitwisselen tussen toezichthouders, politie en OM.
Dat wetenschappelijk onderzoek moet de vraag beantwoorden onder welke voorwaarden, verband houdend met de Europese en Nederlandse wetgeving tot bescherming van persoonsgegevens een structurele uitwisseling van toezichtgegevens mogelijk is. Bijzondere aandacht moet daarbij uitgaan naar de rol van geheimhoudingsverplichtingen in het fiscale recht, het financieel bestuursrecht en het gegevensbeschermingsrecht voor politie en justitie. Verder zal gezocht moeten worden naar een zekere symmetrie in de informatiepositie van politie en justitie enerzijds en bestuursorganen en toezichthouders anderzijds, zonder dat afbreuk wordt gedaan aan de onderzoeksbelangen. Het belang van de bestrijding van fraude en andere vormen van criminaliteit rechtvaardigt dat. Ook zal enige aandacht moeten uitgaan naar de grensoverschrijdende aspecten hiervan. Voor dit onderzoek is thans financiering beschikbaar. Het zal in de loop van 2011 worden gestart en afgerond.

Helpdesk voor professionals in veiligheid en justitiële jeugdzorg

Met de inrichting van een helpdesk voor professionals in de sector veiligheid en justitiële jeugdzorg is in januari 2011 een begin gemaakt. Dit Servicecentrum zal op vraaggedreven wijze ondersteuning gaan geven aan de professionele praktijk. Daarbij moet met name worden gedacht aan de behandeling van meer ingewikkelde gegevensbeschermingsvraagstukken op het snijvlak van rechtshandhaving, bestuur en jeugdzorg, zoals zogeheten casusoverleggen en de veiligheidshuizen. Het werken in samenwerkingsverbanden waarin politie en openbaar ministerie deelnemen leidt in de regel tot de toepassing van verschillende privacywetten. Het verstrekken van gegevens aan en door deze verbanden vergt afwegingen van gecompliceerde aard, waarbij een bepaalde vorm van expertise moet worden ontwikkeld. Het Servicecentrum zal gezamenlijk met de professionals producten ontwikkelen die hen in staat stellen zelfstandig afwegingen te maken over veiligheid, de bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens. Daarmee wordt tevens uitvoering gegeven aan de in het kabinetsstandpunt naar aanleiding van het rapport van de Adviescommissie veiligheid en de persoonlijke levenssfeer en de evaluatie van de Wbp aangekondigde maatregelen ten aan zien van het beter monitoren van de voorwaarden waaronder de verstrekking van persoonsgegevens in samenwerkingsverbanden plaatsvindt. Het Servicecentrum moet op 1 januari 2012 volledig operationeel zijn.
Overigens gelden als goede basis voor het inrichten van een samenwerkingsverband de volgende zes stappen: het bepalen van a. de taken en belangen b. het doel van het delen van informatie, c. de desbetreffende gegevens d. de vorm en inhoud van het delen, e. de verantwoordelijke f. afspraken over hoe en wanneer de verantwoordelijke de betrokkene van informatie voorziet. Het Ministerie van Veiligheid en Justitie is voornemens deze criteria in het vervolg

strikt toe te passen in alle samenwerkingsverbanden waarin het ministerie zelf participeert.

Privacy Impact Assessments

Een Privacy Impact Assessment (PIA) biedt inzicht in de risico's van een verwerking van persoonsgegevens. Wanneer die risico's bekend zijn, kunnen maatregelen worden genomen om deze te beheersen. Er bestaat in Nederland geen verplichting tot het uitvoeren van een PIA. Een PIA heeft de meeste waarde wanneer deze in de ontwerpfase van een gegevensverwerking wordt uitgevoerd. Er bestaat noch op EU-niveau, noch in Nederland een vaststaand model of algemeen aanvaarde methodiek voor het uitvoeren van PIA. In afgelopen jaren is naar aanleiding van een initiatief van het Cbp gebleken dat de gedachten voor het ontwikkelen van een uniforme methodiek voor het uitvoeren van een PIA sterk uiteenlopen. Het bedrijfsleven was van oordeel dat de voorgestelde systematiek te ingewikkeld en te omvangrijk was en is niet langer bereid het initiatief te ondersteunen. Het bedrijfsleven werkt inmiddels aan de ontwikkeling van een privacy risicoscan, toegesneden op de eigen behoeften.
Wat de overheid betreft, vormt het hierboven vermelde wetsvoorstel voor ANPR een goede gelegenheid te bezien op welke wijze de effecten van de voorgenomen maatregelen op de bescherming van de persoonlijke levenssfeer zo goed mogelijk in kaart kunnen gebracht en transparant worden gemaakt. De verwachting is dat de ervaring die daarbij wordt opgedaan van nut kan zijn bij het verder ontwikkelen van PIA's voor eventuele nieuwe gegevensverwerkingen op het werkgebied van het ministerie van Veiligheid en Justitie.
Naar aanleiding van een vraag van de leden van de fractie van D66 op het algemeen overleg van 17 februari 2011 over de JBZ Raad van 24 en 25 februari 2011 naar aanleiding van PIA's, oordeelt het kabinet dat er onvoldoende reden is om het gebruik van PIA's in wetgeving voor te schrijven. Bedacht moet worden dat met het houden van een PIA de nodige kosten zijn gemoeid. Die kosten moeten in een aanvaardbare verhouding staan tot de risico's die met een PIA in kaart kunnen worden gebracht. Het is aannemelijk dat het houden van een PIA voor het midden- en kleinbedrijf relatief vaak zal leiden tot een onevenredig zware verplichting.

Privacy by design

Privacy by design is een goede manier om privacybescherming concreet vorm te geven in informatiesystemen waarin persoonsgegevens worden verwerkt. Door toepassing van privacy by design wordt gegevensbescherming van meet af aan "ingebakken" in het systeemontwerp. Hoewel deze gedachte al geruime tijd bekend is, vindt deze in Nederland nog niet grote schaal toepassing. Het kabinet wil de toepassing van privacy by design stimuleren. Daarvoor is kennis van de kansen en de belemmeringen voor de toepassing noodzakelijk. Het ministerie van Economische Zaken, Landbouw en Innovatie heeft TNO gevraagd hiernaar onderzoek te doen. Dat onderzoek heeft tot doel na te gaan welke drijvende en remmende krachten van invloed zijn op de beslissing van bedrijven om al dan niet over te gaan op informatiesystemen die privacyvriendelijk zijn ontworpen. Het is noodzakelijk meer inzicht te krijgen in de kosten en de baten van privacy by design, in de vraag of dat in het buitenland anders ligt dan in Nederland en in de vraag wat de overheid eraan kan bijdragen om toepassing van privacyvriendelijke systeemontwerpen te bevorderen.

De bescherming van persoonsgegevens op andere terreinen dan veiligheid

In het kabinetsstandpunt heeft het vorige kabinet een visie gegeven op de evaluatie van de Wbp en de gevolgen die het daaraan verbond. In de inleiding van de brief is reeds aangegeven dat dit kabinet die visie in grote lijnen onderschrijft. Dat geldt in beginsel ook voor de in die brief aangekondigde aanpassingen van de Wbp.
Het kabinet ziet in de mededeling van de Commissie overigens aanleiding om een aantal voornemens die zijn neergelegd in het meergenoemde kabinetsstandpunt naar aanleiding van de evaluatie van de Wbp en het rapport van de Adviescommissie veiligheid en de persoonlijke levenssfeer vooralsnog niet in de vorm van Nederlandse wetgeving ten uitvoer te leggen.
Het betreft hier met name de uitwerking van het accountabilitybeginsel in de Wbp (daaronder verstaat het kabinet het stimuleren van het opzetten of uitbreiden van een eigen intern privacybeleid door ondernemingen bij wijze van zelfregulering, in ruil voor het verlichten van administratieve lasten; het bedrijfsleven zou daarbij in de visie van het kabinet optimale keuzevrijheid moeten hebben met betrekking tot de wijze waarop dit beleid wordt ingericht; wellicht is dit ook voor de overheid denkbaar), de ontwikkeling van een zelfstandig klachtrecht voor betrokkenen, zowel binnen als buiten het verband van zelfregulering, en de ontwikkeling van een eigen Nederlandse regeling voor zogeheten Binding Corporate Rules (gegevensbeschermingsregelingen die gelden binnen een concern).
De reden daarvoor is dat de mededeling nadere beleidsvorming door de EU in het vooruitzicht stelt op die onderdelen. Dat beleid is thans nog onvoldoende ontwikkeld, onder meer omdat over de genoemde punten tussen de lidstaten nog verschillend wordt gedacht Wanneer in Nederland op die terreinen op dit moment wetgeving in voorbereiding wordt genomen is het risico te groot dat dit leidt tot interferentie met de voornemens van de Commissie op dat punt.
Dat neemt uiteraard niet weg dat het kabinet bij de komende herziening van de richtlijn inzet op de ontwikkeling van deze instrumenten die het bedrijfsleven veel te bieden hebben en die daardoor ook belangrijk kunnen bijdragen aan een betere naleving van richtlijn en wet.
Op een aantal andere onderdelen lijkt het risico van interferentie van de Nederlandse wetgevingsvoornemens met die van de Commissie minder groot. Het kabinet zal overigens een wetsvoorstel dat thans in voorbereiding wordt genomen gelijktijdig met een consultatie ook voorleggen aan de Europese Commissie om samenloopproblemen zoveel mogelijk te voorkomen en te voldoen aan de verplichtingen van de notificatierichtllijnen

Reactie op de brief van de Vaste Commissie voor Binnenlandse Zaken van 15 februari 2011

Bij bovengenoemde brief vraagt de Vaste Commissie voor Binnenlandse Zaken om een reactie op het artikel "Netherlands - Privacy Profile", van 24 januari 2011 en afkomstig van www.privacyinternational.org. Dit artikel behelst een adequaat en evenwichtig samengesteld overzicht van een groot aantal wetsvoorstellen, vastgestelde wetgeving, feitelijke maatregelen en onderzoeken in verband met wetgeving die allemaal wel een of andere relatie met het onderwerp bescherming van persoonsgegevens of bescherming van de persoonlijke levenssfeer hebben. Het overzicht beslaat een periode van, ruwweg, tien jaar.
Het artikel is niet zelf opiniërend van aard, maar verwijst wel - met bronvermeldingen - naar diverse wetenschappelijke of andere publicaties die dat

wel zijn. Juist omdat het artikel niet zelf opiniërend is, ligt het geven van een inhoudelijke reactie niet voor de hand.